Why your cold email lands in spam, and the three records that fix it

Since February 2024, Gmail and Yahoo filter bulk senders who fail SPF, DKIM or DMARC, or who let spam complaints climb past 0.3 percent. Here is the setup that keeps cold mail in the inbox.

Published 2026-06-30 · A Mue guide

You wrote a tight cold email, sent it, and it never landed. The copy is usually not the problem. The receiving server decided it did not trust your domain before it read the subject line.

What changed in 2024

In February 2024 Gmail and Yahoo turned long-standing best practice into a requirement, and through 2025 they tightened enforcement from soft filtering to outright rejection. A sender who pushes more than 5,000 messages a day to Gmail addresses is a bulk sender, and that status sticks once you cross it. But the three records below are now the baseline every sender is judged against, not just the high-volume ones.

The three records that build trust

- SPF lists which servers may send for your domain. There is one SPF record per domain, so if one exists you merge into it rather than publishing a second.
- DKIM signs each message with a private key your provider holds, against a public key you publish in DNS. The receiver verifies the signature, so it knows the mail was not forged. The key comes from your sending provider, which is why no honest tool can generate it for you.
- DMARC ties the two together: it tells receivers what to do when SPF or DKIM fail and where to send reports. It is the record that turns the other two from advisory into enforced, and it must align with the domain in your From address.

Start DMARC at p=none, then tighten

The common mistake is jumping straight to an enforcing policy. Start at p=none: it blocks nothing but collects reports, so you can see every source sending as you, including ones you forgot. Once SPF and DKIM pass cleanly for a week or two, move to p=quarantine, then to p=reject. The tool builds all of this from your inputs.

The number that actually filters cold senders

Authentication gets you to the door; your complaint rate decides whether you stay. Google asks senders to keep spam complaints below 0.1 percent and says they should never pass 0.3 percent, which is 3 complaints per 1,000 delivered messages. Yahoo points to the same 0.3 percent ceiling. A cold list complains more than an opted-in one, so this is the line most cold

campaigns trip, not the authentication.

Separate domain, slow warmup

- Never send cold outreach from your main brand domain. Use a lookalike domain bought for the purpose, authenticate it, and redirect it to your real site, so a burned reputation never reaches your invoices and customer replies.
- Warm it before you send for real. A new domain that suddenly sends hundreds of cold emails looks exactly like a spammer. Start with a trickle, ramp over several weeks, and stop to clean your list the moment bounces climb past a few percent.
- Add a one-click unsubscribe. Gmail, Yahoo and Apple now expect RFC 8058 one-click unsubscribe on bulk mail, and an easy exit is also the cheapest way to keep complaints under the 0.3 percent ceiling.

One honest caveat

This is a deliverability setup, not legal advice. Landing in the inbox and being allowed to email someone are different questions: under GDPR and similar rules you still need a lawful basis to contact a cold prospect. Get that right first, then use the records above so the mail you are allowed to send actually arrives.

Build your records

The tool generates ready-to-paste SPF, DKIM, DMARC and BIMI records from your inputs, scans a draft for the words filters punish, and lays out a conservative 30-day warmup ramp. Everything is generated in your browser.

Frequently asked questions

Why do my cold emails land in spam even though the copy is fine?
In most cases it is authentication, not wording. Since February 2024 Gmail and Yahoo expect every sender to pass SPF and DKIM and to publish a DMARC record that aligns with the From domain. If any of those is missing or misaligned, the receiving server distrusts the message before it reads a word, and a brand new sending domain with no warmup history makes that distrust worse.

Do the Gmail and Yahoo rules apply to cold email at low volume?
The formal bulk-sender threshold is more than 5,000 messages a day to Gmail addresses, and once a domain crosses it that status is permanent. But SPF, DKIM and DMARC are now the baseline mailbox providers expect from everyone, and the spam-complaint limits hit cold senders hardest because a cold list complains more than an opted-in one. Treat the rules as the floor, not a volume you can stay under.

What spam complaint rate gets you filtered?
Google asks senders to keep the complaint rate below 0.1 percent and says it should never pass 0.3 percent; Yahoo also points to 0.3 percent. That is 3 complaints per 1,000 delivered messages. Cold outreach reaches that ceiling fast, which is why list quality and a clear unsubscribe matter more than send volume.

Should I send cold email from my main company domain?
No. Run outreach from a separate lookalike domain bought for the purpose, authenticate and warm it, and redirect it to your real site. If a campaign draws complaints, the reputation damage stays on the throwaway domain instead of pushing your invoices and customer replies into spam.

Generate your SPF, DKIM and DMARC records

Free, no signup: agent.mue.app/tools/cold-email-deliverability-setup

agent.mue.app/articles/why-your-cold-email-lands-in-spam